ISSN 2522-6398 Vol. 3, Issue 5: 42-48, DOI: 10.25236/FER.2020.030509

The Exploration and Research of the Network Security Offense and Defense Laboratory Cooperated by Schools and Enterprises under the Background of New Engineering

Hao Zhang

Department of Information Technology, Wenzhou Polytechnic, Wenzhou 325035, China

ABSTRACT. *The proposal of new engineering subjects will lead the engineering education of schools into a whole new stage, and schools have joined the ranks of consciously exploring the research and practice of new engineering subjects. The new engineering department is committed to creating engineering talents that adapt to emerging industries and new economic models. Under this background, schools should actively explore new models of school-enterprise cooperation. As a joint co-constructed laboratory for routine projects of school-enterprise cooperation, it has a deeper function in the context of new engineering. This article first discusses the proposal of the new engineering and the new functions of the school-enterprise joint laboratory under this background. Taking the construction practice of the research of the Network Security Offense and Defense Laboratory Cooperated by Schools and Enterprises as example，this article describes the local universities and enterprises jointly build the content and development vision of the innovation laboratory.*

KEYWORDS: *New Engineering, Network Security Offense and Defense Laboratory*

1. Introduction

“Without cyber security, there will be no national security; without informatization, there will be no modernization.” The importance of cyber security has risen to an unprecedented level. With the rapid development of communication technology, today's society has entered the era of Internet of Things. The Internet is already the foundation of the entire society. With the widespread application of information and big data, modern society has entered the digital age. Network security and information security are closely related to national security, social stability, and economic development, and are of vital importance. In 2015, the Ministry of Education added a first-class discipline of “cyberspace security”, and the “Cybersecurity Law” came into effect on June 1, 2017. It is estimated that there are millions of cybersecurity professionals in China.

At present, it is an indisputable fact that there is a serious vacancy in Internet security personnel. Before 2018, several local schoolshave not set up an information security major. Only the computer network major of the vocational and technical college where the author is located has set a security direction. It can train more than 20 students in the network security direction for the society every year. So far, many local colleges and universities, including the vocational and technical colleges where the author is located, have started enrollment of information security-related majors in 2019. The professional name corresponding to higher vocational education is called “Information Security and Management Specialty”, training in information security deployment and implementation, information security High-quality technical skills for management and service.

For the establishment of new majors and the formulation of talent training programs, schoolswill invest in strengthening the construction of relevant laboratories or training platforms. Because the training of network security talents requires high hands-on skills, are the training programs for such majors reasonable or not? Whether the training is carried out smoothly and whether the training evaluation method is appropriate are directly related to the training effect of the professional. The training link is inseparable from the construction of the experimental environment and the training platform. In this case, it is necessary to study the construction of the laboratory and the training platform. The vocational college where the author is located has built a network security offensive and defensive laboratory through cooperation with network security companies, and has achieved very good teaching results.

2. Problems in the traditional model

The author's original network major has built a network security training room, equipped with 24 stations and two sets of offensive and defensive equipment, and the security direction students complete some professional courses in this training room.

2.1 The experimental case is too old

The original equipment was purchased in 2011 for a long period of time. The equipment and available experimental cases are limited and too old. For example, the host security experiments are based on Windows 2003 or Windows XP. It is seriously out of touch with the current mainstream security issues, which is likely to cause students to lack competitiveness.

2.2 The experiment content is too simple

With the rapid advancement in the security field in recent years, the scope of security has also become wider and wider. The original experimental equipment involved in experimentation and training cannot satisfy students' understanding of a complete safety architecture.

2.3 The experimental operation form is not flexible

Safe research thinking is divergent, and the method of unifying student computers and installing specified software in the laboratory will have certain restrictions and restrictions on student learning. And the original laboratory is not suitable for organizing CTF, offensive and defensive games and other forms of learning.

3. The necessity of joint construction of network offensive and defensive training rooms by schools and enterprises

Outstanding enterprises in the field of cyber security are actively participating in the training of cyber security talents in different forms. Compared with other areas in the IT industry, security companies are particularly proactive in education. The laboratory provides a full set of construction schemes, the enterprise has an experimental training platform with product attributes, the enterprise has comprehensive safety equipment, and even the enterprise has a complete talent training system. It cooperates with the school in three dimensions. At the same time, schoolshave also opened windows for external cooperation in a timely manner, and a more open and effective talent training model has been promoted and explored, which has opened up a number of successful paths for talent training in the security industry. Comprehensively consider the respective appeal points of the school and the enterprise, and create a cooperation model and cooperation plan suitable for both parties. There are both common parts and unique parts, which is conducive to the replication and promotion of the model for the enterprise, and the school is more concerned about the representative and characteristic Part of the personality.

Network information security is a new discipline generated in the digital age. It is an interdisciplinary subject across science, engineering, law, and management. It is an emerging discipline in the context of new engineering. The vocational college where the author is located has started enrolling students from the establishment of the network security direction in the network major to the declaration of information security and management major. In just a few years, the development speed of the network information security field is staggering, and the rapid change just illustrates this field. Being active and young also shows the urgency of the society and industry's demand for schoolsto train network information security talents, but the pain points are also obvious, and education still has the disadvantage of lagging behind to some extent. How to use the advantages of enterprises to effectively improve the quality of personnel training is an urgent need for vocational education. This article attempts to explore how to use the complementary advantages of both parties to improve the quality of talent training from the point of view of how to build a professional laboratory together.

4. Principles of building network security attack and defense laboratory

In order to achieve the goal of network security attack and defense training room construction, the following principles should always be adhered to in the design and construction of the laboratory, considering the development of network security technology comprehensively:

(1) Standardization and openness. Communication protocols and interfaces conform to international standards. The support of the international standard network protocol, international standard open protocol, to ensure the smooth connectivity between other networks. Convenient access to different manufacturers of equipment and network products, business integration and data centralization.

(2) High reliability. Network experiment system is stable and reliable application system is the premise of normal operation of the guarantee, selects high reliability network product in network design, network structure, reasonable design and reliable network backup strategy, guarantee the network has the ability of fault self-healing, makes the network under the condition of high load still has high capacity and efficiency, and low latency.

(3) Progressiveness. As the most cutting-edge discipline and technology research place, the school requires the network laboratory to be equipped with the most advanced network equipment, able to carry out the latest technology of scientific research, teaching and practice activities, network laboratory equipment, network solutions of technical advancement requirements are very high.

(4) Manageability. Centralized network monitoring, decentralized management, and uniform distribution of broadband resources.Choose advanced network management platform, with equipment, software, interface management, traffic statistics and analysis, and can provide automatic fault alarm.The entire laboratory platform can be remotely controlled.

(5) Flexibility and extensibility. Depending on future business growth and changes, the network can be expanded and upgraded smoothly, minimizing adjustments to the network architecture and existing equipment.

(6) Security. A unified security policy is formulated to consider the security of the experimental platform as a whole.Through the business subnet isolation, unified planning, according to different business subnet division.Have the ability to ensure the system security and prevent the system from being vandalized.

(7) Comprehensiveness and unity. A network lab is required to complete many different experiments in a network security course.

5. The key points of building a network offensive and defensive training room

(1) Laboratory infrastructure and layout: The laboratory structure is divided into student experiment area, teaching demonstration area, safety service work area and reception area. As shown below.

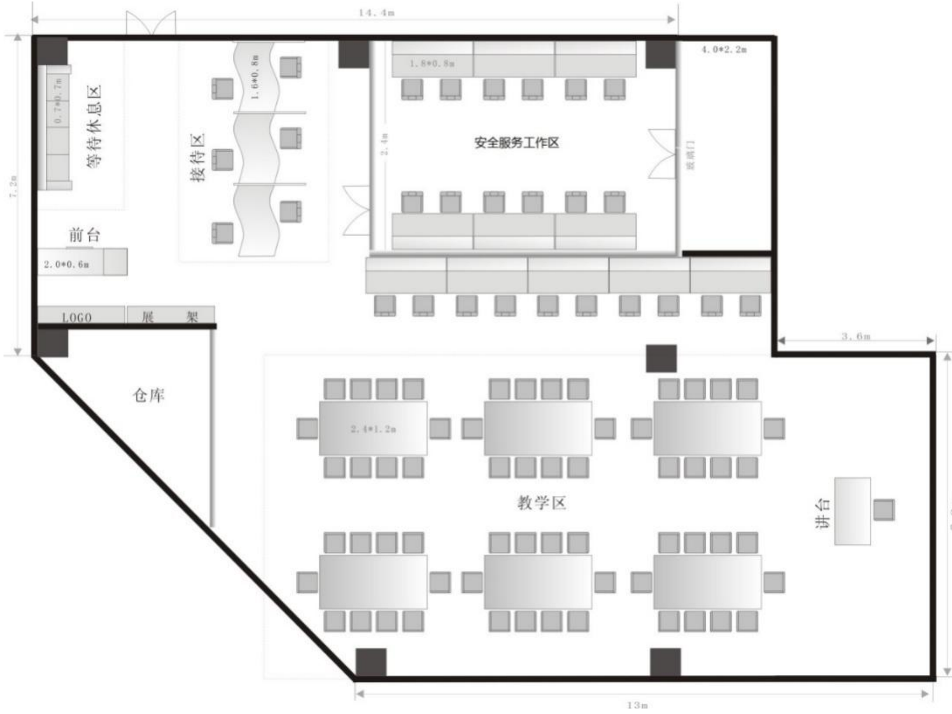

Figure. 1 Network offensive and defensive training room

Among them, 48-60 stations are deployed in the student experimental area, which is divided into 6 groups, 8-10 people in each group. In addition to class or training, the experimental area can also be used to organize the CTF flag capture or attack and defense competition; security service work area 12 stations are deployed for external network security service work and technical research; multiple machines are deployed in the teaching demonstration area to install the consoles of all security devices to realize the management of security devices and to conduct network information security experiments, Centralized demonstration of security offensive and defensive; reception area enables customers to wait and negotiate.

(2) Hardware equipment planning: relatively complete course platform for security vendors, practical training experimental platform for security vendors, network security operation and maintenance equipment of different vendors, iso-guarantee toolbox, situation awareness platform, joint construction of offense and defense experimental platform and target aircraft, A few network devices (to form multiple sets of LANs). According to the different teaching, research, development and other services of the laboratory, a comprehensive basic hardware platform is provided.

(3) Mechanism construction: A perfect mechanism is the basis for ensuring the smooth progress of school-enterprise cooperation. Based on the principles of mutual benefit and win-win, resource sharing, complementary advantages, and common development, the two sides strive to build a long-term mechanism for cooperative development. Through cooperative development and operation mechanisms, a mutually beneficial and win-win mechanism and a coordinated linkage mechanism, the two parties have built a good, co-managed and shared situation. Establish a collaborative education mechanism and collaborative innovation mechanism to enable enterprises to participate in personnel training throughout the process and build an all-round multi-level innovation and entrepreneurship education environment. Establish a flexible employment mechanism, realize the free flow of talents in enterprises and schools, and train and cultivate a “three-energy” (capable of teaching, operational, scientific research) talent team.

(4) Construction of training resources: based on the connection of “talent training goals and industry enterprise talent standards, teaching activities and enterprise production process, teaching content and enterprise typical work tasks, training projects and enterprise job typical positions, training environment” Connect with the production environment of the enterprise, curriculum evaluation and enterprise operation norms and quality standards, connect the training base culture and enterprise culture “, build a complete practical teaching system for professional groups, formulate teaching and assessment standards, and focus on professional quality training.

(5) Construction of the teaching staff: Relying on the resources of enterprises and schools, and with the help of a good mechanism for the exchange of talents between schools and enterprises, it has effectively promoted the sharing and utilization of talents. Through the mutual assignment and assistance of school and enterprise personnel, a team of practical training guidance (project teaching) teachers will be built together.

(6) Service capacity building: The combination of schools and enterprises enables the training platform to realize functions such as “talent cultivation, vocational and skill training, and security services”, and provides students with a basic training environment and further incubation support for innovation and entrepreneurship.

6. Network attack and defense laboratory construction concept

Objective: Due to the destructive nature of network information security and offensive and defensive technologies, network security vulnerabilities set up for teaching can create huge risks. Experiments such as cyber attacks and virus injections in real network environments will have devastating consequences. The establishment of the network offensive and defensive laboratory is mainly aimed at the application of network offensive and defensive technology, mainly to promote the success of security offensive and defensive, realize the experiment in the simulation environment, do a good job with the production network isolation, and do a good job in Internet application security Management, showing threats and vulnerabilities, and managing security risk threats, vulnerabilities, good training and offensive and defensive experiments, better information system security assessment, and better production system penetration testing.

Necessity of establishment: In order to gain a deeper understanding of information security threats and their loopholes, it is necessary to promote the continuous improvement of their information security prevention skills. Therefore, it is necessary to establish a scientific information security laboratory. Its main functions are: centralized management of information security threats and management of information security vulnerabilities in specific areas; visual information security threats in specific areas indicate or display the vulnerability; establish a special attack and defense drill environment as needed to support information security attack and defense drills, especially Have specific requirements; provide certain training and experiments for the specific needs of information security offensive and defensive technologies; demonstrate information security attack experiments to learn more about information security; provide a dedicated research and learning experiment platform.

Part of the cybersecurity offense and defense laboratory

Overall architecture: The network security attack and defense laboratory mainly includes basic network, online course learning platform, experimental training platform, target machine system, competition platform, website security detection platform, vulnerability demonstration platform, etc. Among them, the basic network is mainly to interconnect the experimental network platform according to different experimental network requirements. This operating platform is mainly used for network deployment of both the offensive and defensive parties, and provides terminals for system operation or of the offensive and defensive parties to access their own devices. The online course learning platform is mainly to provide learners with online learning channels. The experimental training platform is mainly to cooperate with the learning of the course learning platform while using experiments to verify. The target system provides an application system that simulates the actual environment. The competition platform is mainly used for CTF flag capture or offensive and defensive matches.

The basic network components mainly include routers, layer 3 switches, layer 2 switches, and firewalls.

Online course learning platform: The online course learning platform is a security company that divides knowledge points into one module according to the reserve of talent knowledge, allowing learners to log in through authorization, which is mainly used for learning. The experimental training platform is a security company's control knowledge module, which simulates the experimental environment and allows learners to log in through authorization. It is mainly used for experimental operations and exercises. The software tools required for the experiment are already built in.

Target system: Network information security and offensive and defensive experiments have special environmental requirements. For example, in the actual network attack and defense experiment, the experiment includes network construction, environment configuration, attack target customization, data processing, protection, and comprehensive penetration testing. The construction of the experimental environment is not only technically demanding but also difficult. Therefore, it is difficult to build a real network offensive and defensive experiment system, and the construction and maintenance costs are high. Therefore, at present, with the help of the Docker container second-level deployment and second-level destruction characteristics, the target machine system is perfectly realized.

Competition platform: After the stage of learning, you need to pass a certain way to test, the more common way is the CTF flag capture or offensive and defensive matches.

The website security detection platform embodies the integration of hardware and software. Real-time monitoring of Web applications using remote monitoring technology, service time is 7 × 24 hours. Through the continuous detection of the website, the website's security protection capabilities and service quality are further improved. The platform's event tracking function can also establish a long-term security guarantee mechanism.

Vulnerability demonstration platform: As an information system, there are generally different loopholes. Mainly include the host, application system and database system. This system adopts virtualization technology, arranges some common vulnerabilities into virtual machine systems by design, and at the same time solidifies these virtual machine systems into an image, which can be restored to the original state by restarting.

7. Main functions of network security attack and defense laboratory

7.1 Cyber Security Technology Training

The network security attack and defense laboratory can create a good teaching and training platform. It is a platform built on virtualization technology, which can conduct professional attack and defense drills and has a special examination system. With this system, you can deepen your understanding of the offensive and defensive process, thereby prompting technicians to better improve their safety skills. This system can be used to show the observer the offensive and defensive process to facilitate their visits and inspections, and can also record the live of the offensive and defensive process for live playback. The platform is very helpful for training and examinations related to information security technology, and should be combined with related training activities such as simulation system security protection exercises. It is very helpful for the cultivation of information security talents, and can carry out activities such as information security awareness education and competitions. The designed teaching training platform will also realize the function of assessment and verification, providing convenience for students. Teachers can also use the system as a platform to evaluate students ’experiments.

7.2 Cyber Security Offensive and Defensive Confrontation Exercise

Network security attack and defense laboratory construction can carry out security attack and defense confrontation drills. The offensive and defensive exercises carried out by the offensive and defensive parties are mainly applied to the simulation platform. The attacker can use all available means or tools to attack the target system. Defenders can use detection and defense systems to resist, and the means to defend against attacks also include security hardening information systems. Information security offensive and defensive confrontation exercises are a very effective method, mainly used to assess the security defense and attack capabilities of information systems, and can also be a good way to verify whether information systems are safe.

7.3 Penetration test

In order to conduct a risk assessment of the production system, it is necessary to conduct penetration testing. The Security Attack and Defense Lab has created such an interface that testers can use the lab ’s attack system to conduct penetration tests, or use the attack system to monitor and evaluate the test. The concept of information security attack and defense laboratory proposed in this article is relatively complete in this respect. Some interfaces can be directly connected to the Internet network. Penetration test engineers can use some tools provided by the laboratory to conduct penetration tests, such as scanning application system weaknesses and database weaknesses. There are two benefits of using the laboratory to conduct penetration testing on production systems: first, the laboratory has more comprehensive scanning and testing tools; second, there are different information security vulnerabilities and threats in the laboratory, including verification of the laboratory environment. These conditions are very helpful for the implementation of penetration testing.

7.4 Safety verification

The information system targeted by safety verification is mainly for the safety assessment of the entire life cycle. The work it involves is mainly the evaluation work, including the acceptance test of the information system, the evaluation before going online and the production environment. In general, the evaluation of the information system before it goes online is mainly the upgrade and reconstruction of the safety evaluation of the operating environment system before and after it is put into operation, and at the same time, it assists in its security enhancement to ensure that the system can be operated online to meet related safety Claim.

7.5 Proof of concept of information security threats and vulnerabilities

It is usually easy to understand that information and information technology have security risks. However, ordinary people often cannot intuitively understand and understand the threats and vulnerabilities of information technology. The offense and defense exercise platform can well verify the concepts of information security threats and vulnerabilities. Attack path and specific operation methods can also be presented more intuitively. Through the intuitive presentation of the offense and defense platform, visitors can be encouraged to have a more intuitive understanding of some abstract content, such as threats, vulnerabilities, and principles of action.

8. Curriculum design of security attack and defense laboratory

Both the school and the enterprise aim at cultivating application-oriented, skill-based and compound information security professionals, and determine the professional training objectives by analyzing information security professional posts, typical job tasks and professional abilities. On the basis of professional positions, this paper makes an in-depth analysis of the commonness and difference among various positions in the professional positions group and the commonness and difference of courses, so as to form a curriculum system at the three levels of general foundation, professional platform and job orientation.

The first stage: network security basic knowledge learning and practice. Students learn the basics of network security mainly in the laboratory. The spiral arrangement is selected, that is, the curriculum is arranged in a circular way, so that the students' knowledge and skills are in a spiral.

The second stage: network security comprehensive training stage. The ultimate learning purpose of information security course is to take precautions against the existing security risks and threats, and in case of its outbreak, it is necessary to timely adjust the security strategy to achieve the goal of minimizing losses. Therefore, it is necessary to be familiar with various attack methods and corresponding defense methods through a lot of practical operation.

The courses mainly cover information security, attack and defense, web attack and defense, penetration testing, information security management, security product management, operation and maintenance, etc., involving the vast majority of courses of network security major. The number of experiments is more than 500, and with the development of network security technology, the experiment content is updated in real time.

The teaching takes students as the main body, takes employment as the orientation, unifies the industry typical job demand and the higher vocational education teaching and the characteristic, highlights the post core ability the core skill curriculum, through the school enterprise cooperation and so on form, constructs has the distinct characteristic curriculum and the teaching material system. Efforts to strengthen the construction of a contingent of teachers, the construction of a school-enterprise joint construction, professional development and reform is an important work of professional construction. Through school-enterprise cooperation, excellent talents can be selected to serve as part-time teachers. Meanwhile, it can strengthen the horizontal joint enterprise technology research and development and professional construction, further clarify the responsibilities of full-time teachers, and strengthen the management and assessment of part-time teachers. We should strengthen professional teachers' enterprise training, practice and learning, emphasize teachers' educational concept of cultivating talents with virtue, improve teachers' information-based teaching ability, and build a professional and high-level teaching team that can adapt to modern higher vocational education.

9. Conclusion

It is proposed that the network security attack and defense laboratory construction mainly depends on network attack and defense technology; it is mainly engaged in web application and database security research, creating necessary scientific research environment and providing convenience for web application, database and host security research and other related security research. Hope that eventually relevant work can be carried out to provide a certain reference.

To build an innovative country, we must comprehensively implement the strategy of rejuvenating the country through science and education and strengthening the country with talents. Talent training is an important foundation for a talented country. The laboratory is the basic condition for talent training and talent display. It is the unremitting pursuit of laboratory management to improve the management level of the network offensive and defensive laboratories and to better serve talent training and talents. The Internet + era has undoubtedly provided direction and goals for this pursuit.

Acknowledgments

Visit engineers' school-enterprise cooperation projects: FG2018065.

The project name: Research and exploration on the practical teaching model of network security laboratory under the school-enterprise co-construction of DAS-WZPT model.

References

[1] In Hong Kong (2010). On the construction of network laboratory in higher vocational colleges [J]. Information Security and Technology, no.9, pp.83-85.
[2] Jian Bin (2010). On the construction of electronic forensics laboratory [J]. Information Network Security, vol.11, no.8, pp.18-19.
[3] Tang Haitao (2010). Talking about the planning and construction of network and information security laboratory [J]. China Science and Technology Innovation Guide, no.10, pp.173-174.
[4] Zhongping (2010). Exploration on the construction of school-enterprise network security laboratory [J]. Laboratory Science, vol.13, no.1, pp.122-124.
[5] Gu Yulin (2008). Research on the construction of enterprise network security laboratory [J]. Baosteel Technology, no.3, pp.74-77.